Cybersecurity introduction

Cybersecurity

2025-2026

Linde Nouwen

KdG

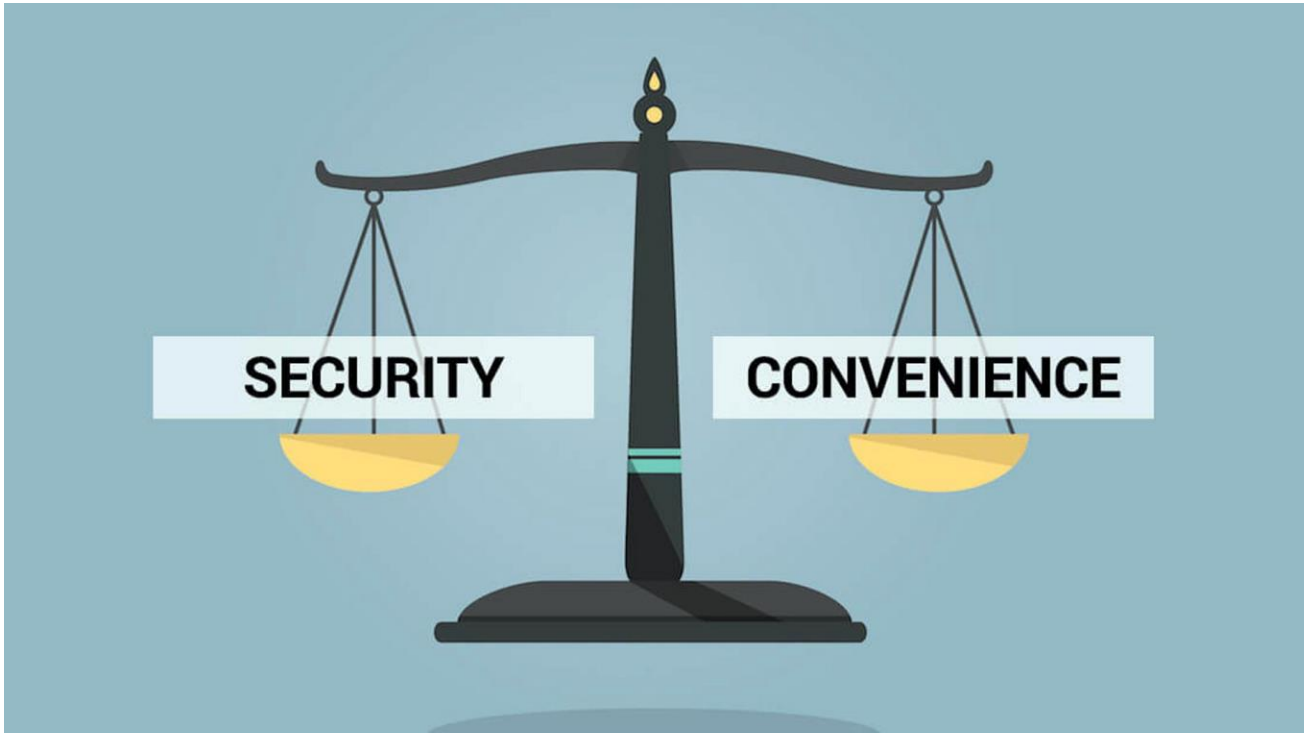
University of Applied Sciences and Arts

Intro

- "The best defense is a good offense"
- Learn to Think & Act like a hacker

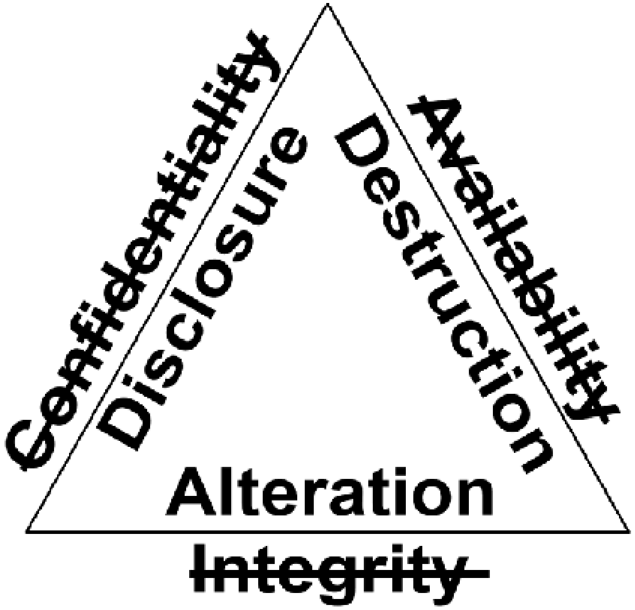
Intro

- The security/ convenience dilemma



Intro

- System-goals:

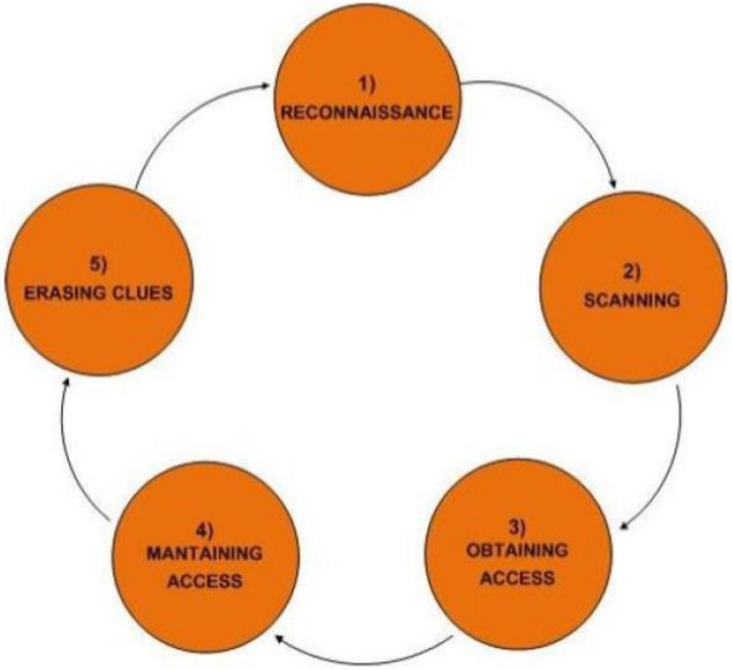


- **Integrity**:maintaining the accuracy, completeness, and trustworthiness of data and systems, ensuring they are free from accidental or unauthorized modification, corruption, or tampering throughout their lifecycle.
- **Availability**:ensures that systems, applications, and data are accessible and usable by authorized users whenever they need them, even during disruptions or attacks.
- **Confidentiality**:the principle of ensuring that data is kept secret and accessible only to authorized individuals or systems.

Methodology

Methodology

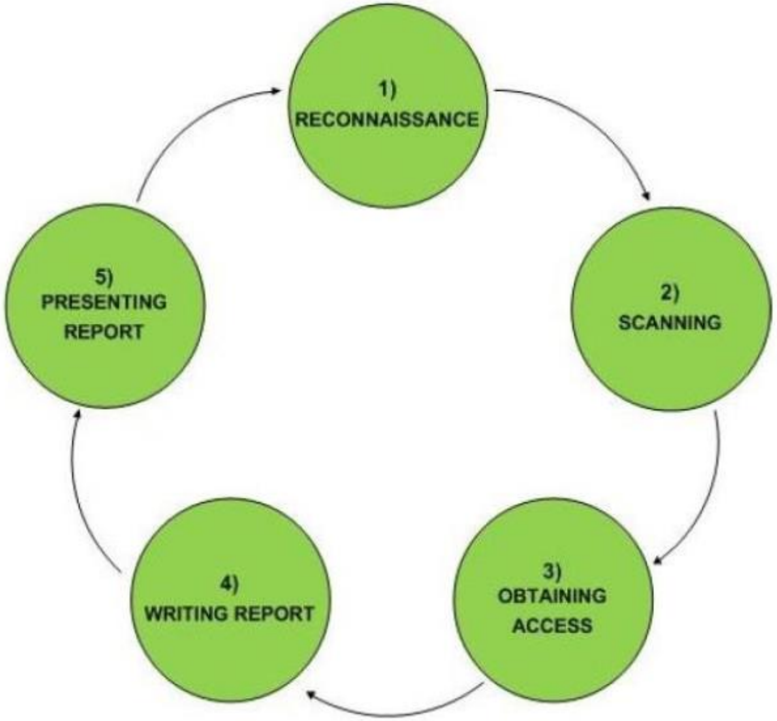
- Malicious hacker



Source: EC-Council

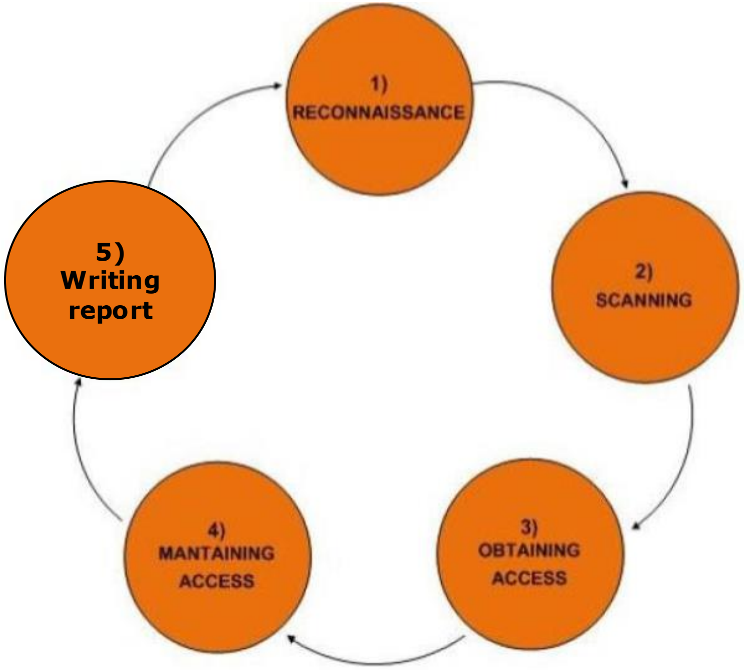
Methodology

- Penetration tester



Methodology

- Red teamer



Source: EC-Council

Terminology

Ethical hacking exercises

- Red teaming
- Purple teaming
- Penetration testing
- Code review
- Config review
- Bug bounty
- …

Types of pentesting

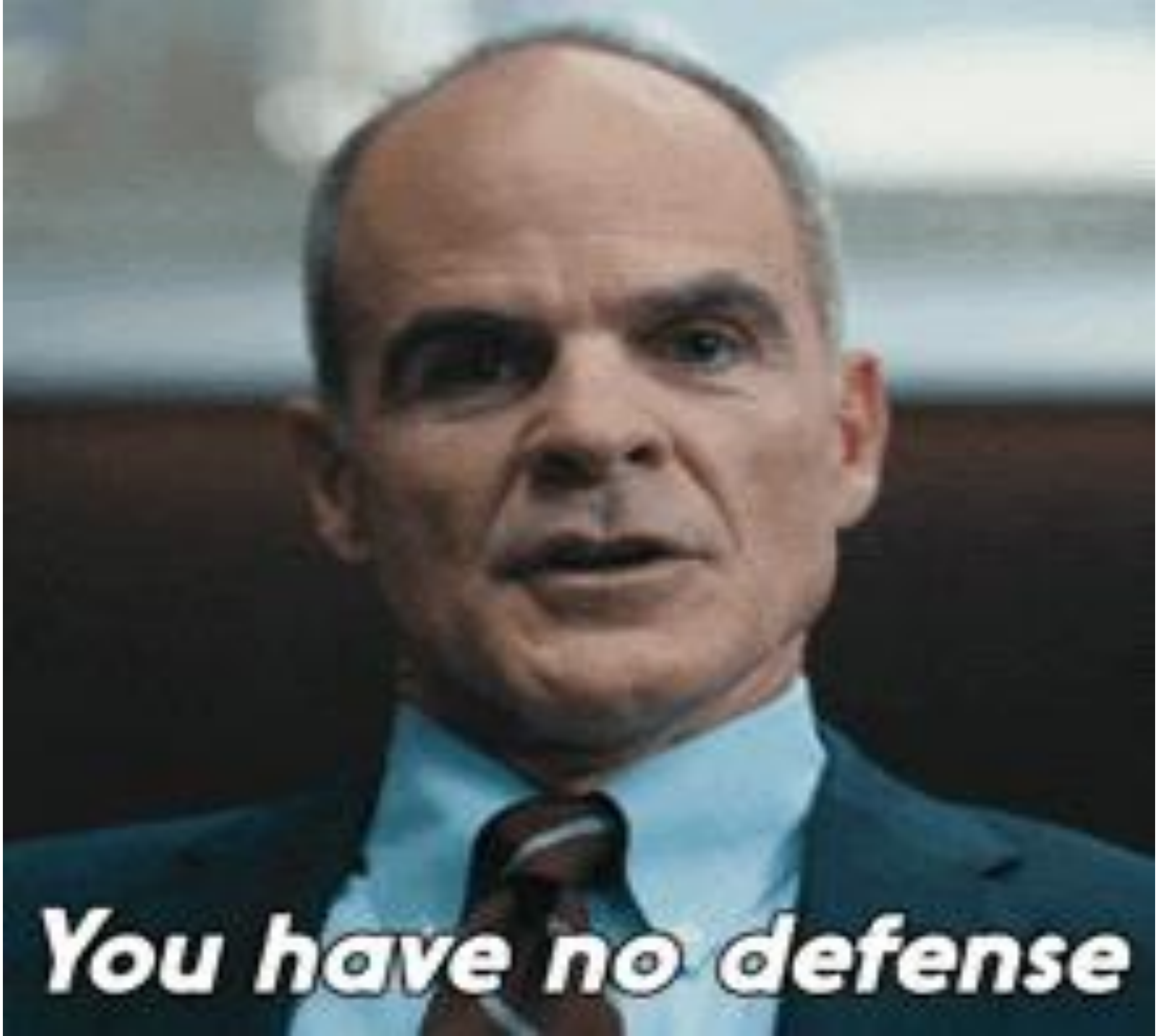
- External pentesting
- Internal pentesting
- Physical pentesting
- Perimeter pentesting
- Web application pentesting
- Mobile application pentesting
- Infrastructure pentesting
- Network pentesting
- ...

Hacking Modes

- Black box
  - External: Organisation name & Let's go...
  - Internal: URL to specific application
- White box
  - Connection and/or access
  - Lots of internal information: schematics, addresses,…
- Grey box
  - In between

Malicious hackers

- Script kiddies
- Suicide Hackers
- Hacktivists
- Nation states
- ...


You have no defense

The blue team

- CSIRT
- SOC
- Threat Intelligence
- Developers
- Network defenders
- Digital forensic analysts
- Vulnerability management

Social engineering

Social engineering

Six key principles of human influence:

1. Reciprocity
2. Commitment and consistency
3. Social proof
4. Authority
5. Liking
6. Scarcity

Methods

- Phishing
- Spear phishing
- Vishing
- Smishing
- Impersonation (eg. Bank at home)

Penetration testing

Why?

- Vulnerability identification
- Compliance with internal policies
- Compliance with external regulation
- Reputation
- Risk management

Key concepts

- **Assets:** What are we protecting? This includes data, intellectual property, hardware, and reputation.
- **Threats:** Who or what is a potential danger? This can be external attackers, insider threats, or even natural disasters.
- **Vulnerabilities:** What are the weaknesses in the system that a threat could exploit? Examples include unpatched software, weak passwords, and misconfigured firewalls.
- **Risks:** The potential for a threat to exploit a vulnerability, resulting in a negative impact. Risk = Threat x Vulnerability.

Pentest methodology

1. Planning: defining the scope
2. Footprinting & Scanning: gather information about the target
3. Enumeration: find running services, users, and potential vulnerabilities
4. Exploitation: exploit vulnerabilities to gain initial access
5. Post-exploitation: privilege escalation, local enumeration, persistence,...
6. Reporting: feedback on the results

Planning

1. Intake meeting
2. Statement of work

What would you ask during the intake meeting?

Intake meeting

- Check for type of test
- Check for test mode
- Verify planned execution
- What is in scope (AND what is out of scope)?
- Which methods are allowed?
- What are the most valuable assets?
- …